

## EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S20	1	"20040131191".pn.	US-PGPUB; USPAT; USOCR	OR	ON	2007/05/03 08:36
S21	61	ibe same public same private	US-PGPUB; USPAT; USOCR	OR	ON	2007/05/03 08:36
S22	69	ibe same public same private	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT ; IBM_TDB	OR	ON	2007/05/03 08:36
S23	2	@ad<"20020705" and ibe same public same private	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT ; IBM_TDB	OR	ON	2007/05/03 08:37
S24	88	@ad<"20020705" and ((identity identifier) adj2 encryption) AND (public same private same generat\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT ; IBM_TDB	OR	ON	2007/05/03 08:37
S25	3	@ad<"20020705" and ((identity identifier) adj2 encryption) AND (public same private same generat\$3) and ((multipl\$5 plural\$3) near2 (ta authority trusted))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT ; IBM_TDB	OR	ON	2007/05/07 14:14
S26	0	@ad<"20020705" and ((identity identifier) adj based adj encryption) AND (public same (private NEAR2 generat\$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT ; IBM_TDB	OR	ON	2007/05/03 08:41
S27	2	@ad<"20020705" and ((identity identifier) adj based adj encryption) AND ((private NEAR2 generat\$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT ; IBM_TDB	OR	ON	2007/05/04 11:04
S28	0	@ad<"20020705" and ((identity identifier) adj based adj encryption) AND ((private NEAR2 generat\$3))	US-PGPUB	OR	ON	2007/05/04 11:04
S29	1	"20030179885".pn.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/04 12:25
S30	1944	(identi\$5 adj based) and processor and generator	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/04 12:27
S31	861	@ad<"20020705" and (identi\$5 adj based) and processor and generator	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/04 12:28

## EAST Search History

S34	1	@ad<"20020705" and (ident\$5 adj based adj \$2crypt\$7) and processor and (key near2 generator)	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/04 12:29
S36	1	"20030179885".pn.	US-PGPUB; USPAT	OR	ON	2007/05/07 09:04
S37	7	boneh.in. and identity	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/07 13:58
S38	41	((LIQUN) near2 (CHEN)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2007/05/07 14:06
S39	3	((DAVID) near2 (SOLDERA)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2007/05/07 14:06
S40	73	((KEITH) near2 (HARRISON)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2007/05/07 14:06
S41	135	((KEITH) near2 (HARRISON)).INV.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT ; IBM_TDB	OR	ON	2007/05/07 14:06
S42	5	((DAVID) near2 (SOLDERA)).INV.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT ; IBM_TDB	OR	ON	2007/05/07 14:06
S43	75	((LIQUN) near2 (CHEN)).INV.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT ; IBM_TDB	OR	ON	2007/05/07 14:06
S44	169	S41 S42 S43	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/07 14:06
S45	63	S44 and (public adj (key parameter))	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/07 14:07
S46	21	S44 and (public adj (key parameter)) and elliptic	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/07 14:07
S47	20	S44 and (public adj (key parameter)) and elliptic and weil	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/07 14:11
S48	12	S44 and (weil tate).clm.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/07 14:12
S49	6	S44 and (weil tate).clm. and identity.clm.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/07 14:12

## EAST Search History

S50	1	@ad<"20020705" and ((identity identifier) adj2 encryption) and (bilinear near3 encrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT ; IBM_TDB	OR	ON	2007/05/07 14:14
S51	0	@ad<"20020705" and ((identity identifier) adj2 encryption) and (bilinear near3 encrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB	OR	ON	2007/05/07 14:15
S52	25	@ad<"20020705" and ((identity identifier) adj2 encryption) and (trusted same secret)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB	OR	ON	2007/05/07 14:16
S53	14	@ad<"20020705" and ((identity identifier) adj2 encryption) and (trusted same secret same (public adj key))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB	OR	ON	2007/05/07 14:16

## EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1249	380/30.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/07 14:42
L2	251	380/286.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/07 14:43
L3	856	380/44.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/07 14:43

[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#) |

Welcome United States Patent and Trademark Office

**Search Session History**[BROWSE](#)[SEARCH](#)[IEEE XPLORE GUIDE](#)

Edit an existing query or  
compose a new query in the  
Search Query Display.

Select a search number (#)  
to:

- Add a query to the Search Query Display
- Combine search queries using AND, OR, or NOT
- Delete a search
- Run a search

**Mon, 7 May 2007, 2:19:47 PM EST****Search Query Display**  
**Recent Search Queries**

#1 (((bilinear <and> encrypt)<in>metadata)) <and> (pyr >= 1950 <and> pyr <= 2003)

#2 (((bilinear <and> public)<in>metadata)) <and> (pyr >= 1950 <and> pyr <= 2003)

#3 (((((weil <or> tate) <and> pairing <and> encryption)<in>metadata)) <and> (pyr >= 1950 <and> pyr <= 2003))

  
[Help](#) [Contact Us](#) [Privacy &](#)

© Copyright 2006 IEEE -

Indexed by  
 Inspec®

[Sign in](#)[Google](#)[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)[Advanced Search](#)[Preferences](#)**Web**Results 1 - 10 of about 72,000 for **bilinear pairing encryption**. (0.13 seconds)**[PDF] Identity-Based Encryption from the Weil Pairing**File Format: PDF/Adobe Acrobat - [View as HTML](#)

Our identity-based **encryption** scheme is presented. in Section 4 using general **bilinear** maps. Then a concrete identity based system from the Weil **pairing** is ...  
[crypto.stanford.edu/~dabo/papers/ibe.pdf](http://crypto.stanford.edu/~dabo/papers/ibe.pdf) - Similar pages

**[PDF] An ID-Based Broadcast Encryption Scheme for Key Distribution**

File Format: PDF/Adobe Acrobat

crypton scheme from **bilinear pairings** is based on a variant of the. Boneh-Franklin identity based **encryption** scheme. Index Terms—**Bilinear pairing**, ...  
[ieeexplore.ieee.org/iel5/11/26766/101109TBC2005847600.pdf?arnumber=101109TBC2005847600](http://ieeexplore.ieee.org/iel5/11/26766/101109TBC2005847600.pdf?arnumber=101109TBC2005847600) - Similar pages

**[PDF] Efficient identity-based multicast scheme from bilinear pairing**

File Format: PDF/Adobe Acrobat

holds a key **encryption** key (KEK). The leaves of the tree. correspond to the group members. ... based on **bilinear pairing**. Our scheme has several desirable ...  
[ieeexplore.ieee.org/iel5/2191/33164/01561965.pdf?arnumber=1561965](http://ieeexplore.ieee.org/iel5/2191/33164/01561965.pdf?arnumber=1561965) - Similar pages  
[ More results from ieeexplore.ieee.org ]

**[Abstract] Efficient Certificateless Public Key Encryption with ...**

Certificateless public key **encryption**; **bilinear pairing**; Key escrow. ... generic series construction model of certificateless public key **encryption** (CL-PKE) ...  
[www.actapress.com/PaperInfo.aspx?PaperID=23663](http://www.actapress.com/PaperInfo.aspx?PaperID=23663) - Similar pages

**[Paper] Efficient Certificateless Public Key Encryption with Pairing**KEY WORDS Certificateless public key **encryption**; **bilinear pairing**; Key escrow. 1

Introduction Traditionally, a Public Key infrastructure (PKI) is used to ...  
[www.actapress.com/PDFViewer.aspx?paperId=23663](http://www.actapress.com/PDFViewer.aspx?paperId=23663) - Similar pages

**Scalable, Server-Passive, User-Anonymous Timed Release Public Key ...**

Scalable, Server-Passive, User-Anonymous Timed Release Public Key **Encryption** from **Bilinear Pairing** (2004) (Make Corrections) Ian F. Blake, Aldar C-F. Chan ...  
[citeseer.ist.psu.edu/713155.html](http://citeseer.ist.psu.edu/713155.html) - 20k - Cached - Similar pages

**[PDF] Chameleon Signature from Bilinear Pairing**File Format: PDF/Adobe Acrobat - [View as HTML](#)

ID-based chameleon hash function based on **bilinear pairing** and build the ... [8] D. Boneh and M. Franklin, Identity-based **encryption** from the Weil **pairing**, ...  
[eprint.iacr.org/2003/238.pdf](http://eprint.iacr.org/2003/238.pdf) - Similar pages

**[PS] Scalable, Server-Passive, User-Anonymous Timed Release Public Key ...**File Format: Adobe PostScript - [View as Text](#)

Timed Release Public Key **Encryption** from **Bilinear Pairing**. Ian F. Blake, Aldar C-F. Chan. Department of Electrical and Computer Engineering ...  
[eprint.iacr.org/2004/211.ps](http://eprint.iacr.org/2004/211.ps) - Similar pages  
[ More results from eprint.iacr.org ]

**[PS] Practical Identity-Based **Encryption** in Multi-PKG Environment from ...**File Format: Adobe PostScript - [View as Text](#)

In this paper, we present a new identity-based **encryption** (IBE) scheme, using **bilinear pairings**. Our IBE scheme enjoys the same Key Extraction and De- ...  
mirror.cr.yp.to/eprint.iacr.org/2007/100.ps - Similar pages

[PDF] **ATTACK ON IDENTITY-BASED BROADCASTING ENCRYPTION SCHEMES\***

**Introduction**

File Format: PDF/Adobe Acrobat

Broadcast **encryption** systems are now more and more popular. A typical ... MSL schemes are based on **bilinear pairing**. Before presenting ...

www.springerlink.com/index/vg842101x3430538.pdf - Similar pages

Result Page:    [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#)    [\*\*Next\*\*](#)

Try [Google Desktop](#): search your computer as easily as you search the web.

---

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)

---

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2007 Google